

# UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
Samsung Cellphone, IMEI: 354241401241189

Case No. 1:23MJ 184

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

47 U.S. Code § 223

Federal Harassing Phone Calls Statute

The application is based on these facts:  
See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Zachary M. Neeffe

Applicant's signature

Zachary M. Neeffe, Special Agent, HSI

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 4/28/2023

  
Judge's signature

City and state: Winston-Salem, North Carolina

The Honorable Joi Elizabeth Peake, U.S. Magistrate Judge  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH  
OF A SAMSUNG CELLPHONE,  
IMEI: 354241401241189

Case No. 1:23MJ 186

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Zachary M. Neefe, a Special Agent with Homeland Security

Investigations, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 for the digital contents of a cellular telephone particularly described as a Samsung Cellphone with IMEI<sup>1</sup>: 354241401241189, seized from the person of Fidencio MONTERO (the "SUSPECT DEVICE"), whose service provider is believed to be T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The SUSPECT DEVICE is described herein and in Attachment A, and the digital contents to be seized are described herein and in Attachment B.

---

<sup>1</sup> An IMEI, or International Mobile Equipment Identity, is a unique number used for the identification of mobile devices, usually observable in the battery compartment of a cellular phone.

2. I have been employed as a Special Agent (“SA”) of the U.S. Department of Homeland Security (“DHS”), Homeland Security Investigations (“HSI”) since February of 2020 and am currently assigned to the Winston-Salem, North Carolina, Office of the Resident Agent in Charge. Prior to working with HSI, I was a detective and federal task force officer for over two years at the Alamance County Sheriff’s Office in North Carolina where I specialized in child exploitation and sexual abuse investigations. I am now in my thirteenth (13) year of combined state/local/federal law enforcement experience.

3. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training facilitated by the Internet Crimes Against Children (“ICAC”) Task Force, at the National Cybercrimes Center (“C3”), the National White Collar Crime Center (“NW3C”), and everyday work relating to conducting these types of investigations. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 47 U.S. Code § 223 (Federal Harassing Phone Calls Statute) and I am authorized by law to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 47 U.S. Code § 223 (Federal Harassing Phone Calls Statute) have been committed, are being committed, and will continue to be committed by Fidencio Montero or a yet-unidentified suspect utilizing Mr. Montero's cellular device. There is also probable cause to believe that the digital information on the seized device as described in Attachment B will constitute evidence of these criminal violations and will lead to the positive identification of Mr. Montero or another individual who is engaged in the commission of these offenses and locations or property designed for use, intended for use, or used in committing or facilitating these crimes.

6. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. In March of 2023, Homeland Security Investigations (HSI) Winston-Salem Special Agent (SA) Zachary Neefe (the affiant) opened an investigation into harassing phone calls / cyberstalking occurring to a victim inside the coverage area of HSI Winston-Salem. I had learned that an adult female in the area was experiencing extreme phone harassment and possibly threats from an unknown male caller. Burlington Police Department (BPD) Detective Kelle Sisk was currently investigating the case; however, she subsequently requested my involvement for federal resources and possible prosecution.

8. After talking by phone with Det. Sisk to arrange a face-to-face meeting date, I met with Det. Sisk and victim G.T. at the Burlington Police Department on March 14, 2023. G.T. appeared sober and of full faculties throughout interaction with law enforcement; however, she was noticeably irritated that there had not been previous action on the part of law enforcement to rectify this situation. I assured her that HSI had not had previous interaction with this case but that I would attempt to bring resolution to the matter.

9. G.T. recounted during a subsequent recorded interview that she had changed phones in January 2021 after moving cross-country from Bend,

Oregon. Once moved, G.T. changed her number to a new number known to your affiant ("Victim Phone Number)." The area code to Victim Phone Number returns to New Jersey where G.T.'s mother was residing. Immediately after obtaining the new number, G.T. stated that she began receiving phone calls, voicemails, and text messages from **732-896-1716** ("SUSPECT PHONE NUMBER"). G.T. stated the calls/messages were creepy in nature- sometimes they were sexual, other times the message (such as a voicemail) would just consist of dead air, other messages or calls consisted of someone talking to someone else in the background. The messages or talking from the SUSPECT PHONE NUMBER consisted of a male-sounding voice speaking Spanish.

10. When asked for clarification on her interaction with the voice, G.T. stated that she asked numerous times for the person to stop calling or leaving messages. Due to the messages sometimes being sexual in nature, such as kissing emojis or other innuendos, G.T. said she feared for her safety in continuing the interaction with this unknown third party. The victim stated that she utilized an app to translate her conversations with the male suspect where she asked repeatedly for him to break off contact. G.T. clarified that she did not know this person and had never said or done anything to encourage the contact. In fact, G.T. stated that she had gotten so mad at one

point that she utilized profanity in an extreme attempt to get the suspect to stop calling her.

11. G.T. also stated during this meeting that other law enforcement officers had encouraged her to just block the SUSPECT PHONE NUMBER and/or change her number. Regarding blocking the number, G.T. stated that her cellphone provider, Verizon, was only able to block the number for 90 days, after which time the suspect would resume calling her. She stated that a Verizon representative had shared that there was no way to implement a “permanent block.”<sup>2</sup> Once the suspect began calling again, G.T. stated the calls would be so frequent that her voicemail would literally fill up in a matter of days. After learning that the SUSPECT PHONE NUMBER was serviced by T-Mobile, G.T. also emailed T-Mobile in an attempt to implement a call block from that end, but the email bounced as undeliverable.

12. Regarding changing her number, G.T. stated that this was unworkable due to current life circumstances. G.T. identified herself as a 9/11 first responder and survivor. As such, she advocates for other victims and

---
























<sup>2</sup> According to Verizon’s website, a customer can block up to five numbers for free, but this block expires after 90 days. *How to Block Numbers, Calls, Ads, Text Messages & Emails*, <https://www.verizon.com/support/block-numbers/> (last accessed April 25, 2023). In order to block a call permanently, the charge is \$4.99 a month. *Id.*

individuals affected by cancers, health conditions, and other survivor concerns. G.T. stated that members of Congress, other victims, and advocacy organizations all have her current number listed as her primary point of contact; thus, changing her number at this point would uproot many of the professional and personal connections that she has made related to 9/11 advocacy.

13. While present at the Burlington Police Department, G.T. signed a written consent (and provided recorded verbal consent) for a limited phone search of her cellular phone. G.T. stated that investigators could search the cellphone with Victim Phone Number for evidence related to this incident. Areas allowed access on the device included: Call records, a photo folder titled "Telephone harassment," text messages, and voicemails. Other evidence provided by G.T. during this initial meeting included a timeline document that she had used to document both calls from the suspect and interactions with police; the Readington Township Police Department Report; Verizon Wireless billing statements for G.T.'s account; and an Immigration & Customs Enforcement (ICE) Enforcement Removal Operations (ERO) contact that G.T. knew who had offered assistance in the event that the suspect was identified as illegally present in the United States.

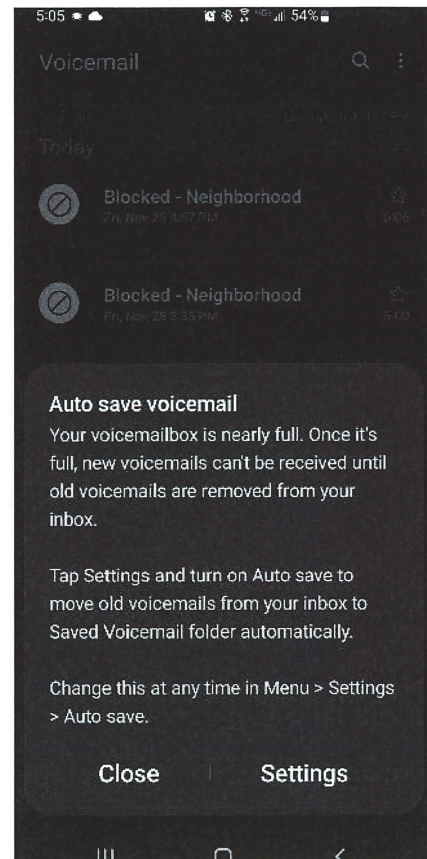
14. Law enforcement and G.T. exchanged contact information and agreed to update one another on the case's status moving forward.

15. Since that time, I have been able to review data on G.T.'s phone and have confirmed her account of events to the best of my ability. The call records on the device indicate that there are 1,984 entries of an incoming call record between G.T.'s phone and the SUSPECT PHONE NUMBER. These phone records run from December 12, 2022, through March 14, 2023, but are incomplete due to being device-specific records. This means that this number

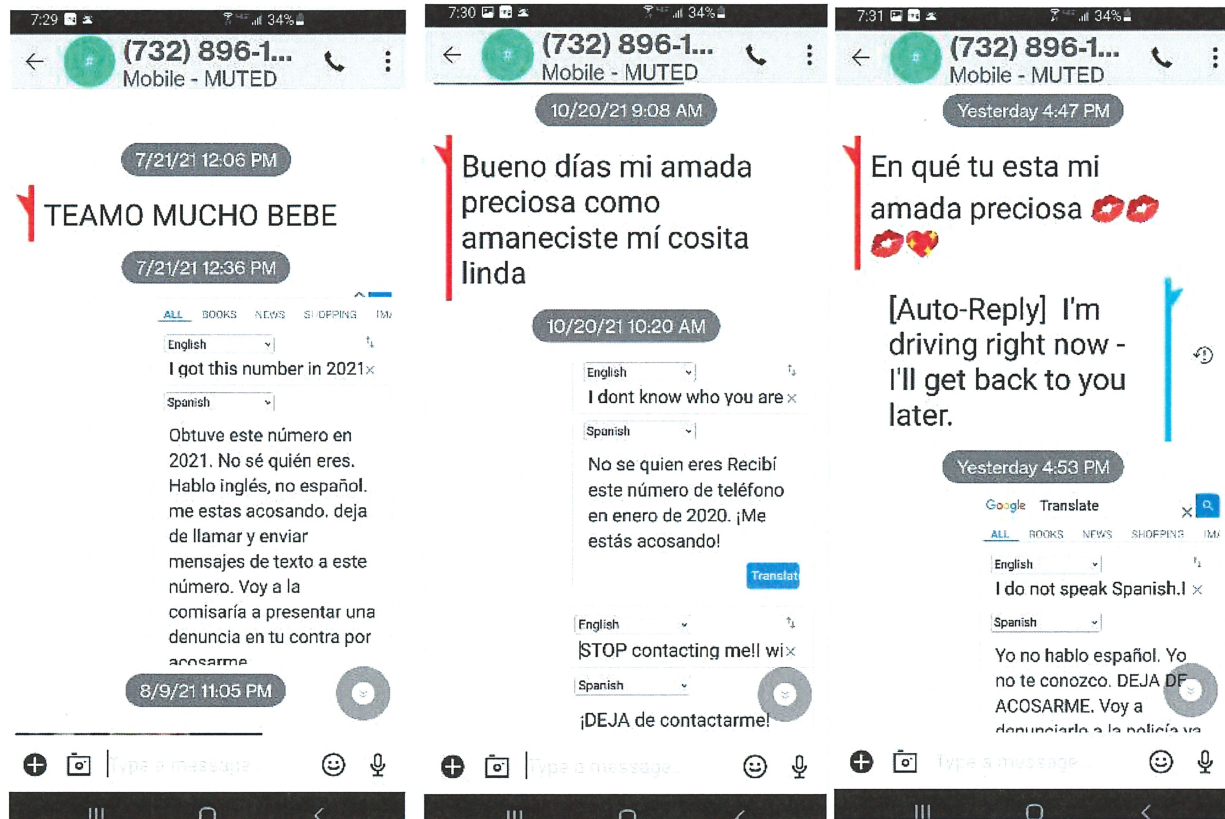
1962					From: 7328961716 Harassment 1/19/21	3/13/2023 10:06:13 AM(UTC-4)	Incoming
1963					From: 7328961716 Harassment 1/19/21	3/13/2023 10:06:23 AM(UTC-4)	Incoming
1964					From: 7328961716 Harassment 1/19/21	3/13/2023 10:06:34 AM(UTC-4)	Incoming
1965					From: 7328961716 Harassment 1/19/21	3/13/2023 11:50:39 AM(UTC-4)	Incoming
1966					From: 7328961716 Harassment 1/19/21	3/13/2023 11:51:01 AM(UTC-4)	Incoming
1967					From: 7328961716 Harassment 1/19/21	3/13/2023 11:51:11 AM(UTC-4)	Incoming
1968					From: 7328961716 Harassment 1/19/21	3/13/2023 5:46:25 PM(UTC-4)	Incoming
1969					From: 7328961716 Harassment 1/19/21	3/13/2023 6:05:26 PM(UTC-4)	Incoming
1970					From: 7328961716 Harassment 1/19/21	3/13/2023 6:24:59 PM(UTC-4)	Incoming
1971					From: 7328961716 Harassment 1/19/21	3/13/2023 7:58:45 PM(UTC-4)	Incoming
1972					From: 7328961716 Harassment 1/19/21	3/13/2023 9:30:21 PM(UTC-4)	Incoming
1973					From: 7328961716 Harassment 1/19/21	3/13/2023 9:30:55 PM(UTC-4)	Incoming
1974					From: 7328961716 Harassment 1/19/21	3/13/2023 9:34:44 PM(UTC-4)	Incoming
1975					From: 7328961716 Harassment 1/19/21	3/13/2023 9:35:05 PM(UTC-4)	Incoming
1976					From: 7328961716 Harassment 1/19/21	3/13/2023 10:19:45 PM(UTC-4)	Incoming
1977					From: 7328961716 Harassment 1/19/21	3/13/2023 10:19:54 PM(UTC-4)	Incoming
1978					From: 7328961716 Harassment 1/19/21	3/13/2023 10:20:03 PM(UTC-4)	Incoming
1979					From: 7328961716 Harassment 1/19/21	3/14/2023 12:16:48 AM(UTC-4)	Incoming
1980					From: 7328961716 Harassment 1/19/21	3/14/2023 12:16:55 AM(UTC-4)	Incoming
1981					From: 7328961716 Harassment 1/19/21	3/14/2023 12:17:03 AM(UTC-4)	Incoming
1982					From: 7328961716 Harassment 1/19/21	3/14/2023 3:47:25 AM(UTC-4)	Incoming
1983					From: 7328961716 Harassment 1/19/21	3/14/2023 3:47:39 AM(UTC-4)	Incoming
1984					From: 7328961716 Harassment 1/19/21	3/14/2023 3:47:48 AM(UTC-4)	Incoming

is likely much lower than the number of calls made to Victim Phone Number as any “blocked” calls would not be reflected in this total. (*See demonstrative screenshot below from phone extraction for call frequency*)

16. Additionally, I have reviewed the phone screenshots taken by G.T. to memorialize text messages and voicemails sent to her. G.T. even made a specific folder on her device titled “Telephone Harassment” to categorize the numerous screenshots that she has taken of messages or activity involving the suspect. All incoming messages appear to be in Spanish and as previously described by G.T., consist mainly of references to love or attraction generally. (*Message at right shows G.T.’s phone displaying a warning about her voicemail inbox being nearly full*)



17. I was also able to use the screenshots to corroborate G.T.'s account of events concerning asking the suspect using the SUSPECT PHONE NUMBER to stop messaging her. G.T. stated that she asked the suspect to



stop contacting her on numerous occasions, even going so far as to send a profanity-laced meme in a last-ditch effort to get him to stop calling/messaging.

- a. *Left Above Screenshot: Suspect says, “I love you very much Baby” or similar, with G.T. using Google Translate to copy/paste a reply into the text field. G.T. responds saying something like, “I got this number in 2021. I don’t know who*

*you are. I speak English, not Spanish. You are harassing me when you call and send text messages to my number. I am going to go to the police station to file a complaint against you for harassing me.”*

b. *Center Above Screenshot: Suspect says something like, “Good morning my lovely beloved. Good morning my cute little thing.” G.T. responds by stating, “I don’t know who you are. I received this telephone number in the year 2020. You are harassing me! Stop contacting me!”*

c. *Right Above Screenshot: The suspect says the following, or similar, “That you would be my precious love.” The message includes lip emojis and a heart emoji. G.T.’s phone is configured to auto-reply when driving. After the auto-reply, G.T. responds by stating, “I do not speak Spanish. I do not know you. Stop harassing me. I’m going to report at the police...”*

18. Although there is ample additional evidence of harassing phone calls, I have not located any threatening or implied threats from the messages from the SUSPECT PHONE NUMBER. G.T. may feel “stalked” or otherwise fearful of the suspect based on the volume of calls/messages but

there does not appear to be overt threats coming from him. Additionally, the phone extraction does not appear to have captured the audio of the voicemails reported by G.T. For this reason, I have not been able to review their contents as of the time of this affidavit.

19. In addition to the digital extraction on the victim's phone conducted with G.T.'s consent, I have examined subpoenaed phone records from both accounts. On March 15, 2023, I served T-Mobile (SUSPECT PHONE NUMBER 732-896-1716) and Verizon (Victim Phone Number) with Department of Homeland Security Summonses for Subscriber Records (similar to an administrative subpoena). T-Mobile provided responsive records on March 24, 2023, and Verizon responded with records on April 3, 2023. Detailed analyses of these records are still pending; however, some of the initial findings are as follows:

- a. From March 23, 2021 (start date for call records from T-Mobile) through March 15, 2023 (end date specified on the DHS Summons), there are quite literally thousands of call records between the two numbers. The T-Mobile spreadsheet shows a total of 75,458 rows total, almost all of which are records pertaining to interaction between the two numbers. These interactions include outgoing calls

“mSOriginating” and “moc”) from the suspect’s phone to Victim Phone Number, and “SMSs”, which T-Mobile denotes as text message records.

- b. Verizon produced records in a different manner, providing both spreadsheets (more-recent call logs) and billing statements (older call records). Thus, an apples-to-apples comparison between the two companies’ records is not possible; however, my initial examination confirms that the call records provided by both companies substantiate the allegations made by G.T.
- c. Of note, the account holder for the T-Mobile (SUSPECT PHONE NUMBER) is listed as “Fidencio Montero”, with billing address 61 Brighton Ave. Perth Amboy, NJ 08861. The account was established September 9, 2020, and was active as of the time of the DHS Summons. The account is a Boost Mobile prepaid account, although the T-Mobile records also list the account as being held through one of their wholesale partners, Dish Network.

20. Fidencio Montero, who is listed as the sole account holder for the the account connect with the SUSPECT PHONE NUMBER, appears to be

Fidencio NMN Montero (H/M, DOB: 02/22/1972). MONTERO is a foreign national, originally from the Dominican Republic, who is currently residing in the United States without lawful legal status. He appears to be a work Visa overstay with minimal online or social media presence.

21. On April 13, 2023, at my request, HSI Newark, New Jersey initiated a surveillance operation around known addresses associated with MONTERO. They were assisted by Immigration & Customs Enforcement (ICE) Enforcement & Removal Operations (ERO) due to MONTERO's illegal immigration status. On this date, HSI Newark & ERO personnel located MONTERO as he left a residence in Perth Amboy, New Jersey. After confirming his identity, ERO personnel took MONTERO into custody on immigration charges, specifically, Section 237A1B of the Immigration and Nationality Act (INA).

22. During the subsequent search incident to arrest, HSI Newark recovered & seized a cellphone from MONTERO's person. This cellphone, particularly described as a Samsung Cellphone with IMEI: 354241401241189 (SUSPECT DEVICE), is the object of this search warrant. HSI Newark has since sent the cellphone to me via common carrier Federal Express ("FedEx") and as of April 20, 2023, I have the SUSPECT DEVICE in my custody, pending lawful authorization to search same.

23. In subsequent contacts with victim G.T., she has stated that since MONTERO's arrest and seizure of the SUSPECT DEVICE, the harassing phone calls and text messages have completely ended. As of April 25, 2023, Montero remains in custody.

#### **MANNER OF SEARCHING COMPUTER SYSTEMS**

24. As described in Attachment B, this application seeks permission to search for records that might be found on the Suspect's Cell Phone in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. *Probable cause.* I submit that since the cellphone was recovered from the suspect's person, and since his arrest the harassing phone calls have ended, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via

the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the

form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Suspect’s Cell Phone because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a

paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further

suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the

computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense

under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other

information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

## CONCLUSION


28. Based upon the specific facts and circumstances outlined in this investigation, there is probable cause to believe that the information associated with the SUSPECT DEVICE contains evidence of violations of 47 U.S. Code § 223; I therefore respectfully request that a warrant be issued for the search of the digital device described in Attachment A for the search and seizure of the items more fully described in Attachment B and request that the Court issue the proposed search warrant.

29. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items seized. Unless otherwise ordered by the Court, the return will not include digital evidence later examined by a forensic analyst.

Respectfully submitted,

/s/ Zachary M. Neefe  
Zachary M. Neefe  
Special Agent  
Homeland Security Investigations

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of the written affidavit.

  
JOI ELIZABETH PEAKE  
UNITED STATES MAGISTRATE JUDGE  
MIDDLE DISTRICT OF NORTH CAROLINA

4/28/2023

**ATTACHMENT A**

**Property to Be Searched**

Samsung Cellphone with IMEI : 354241401241189, seized from the person of  
Fidencio MONTERO (SUSPECT DEVICE), including any storage medium  
contained therein.

## **ATTACHMENT B**

### **Particular Things to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 47 U.S. Code § 223:

1. Records, information, and items relating to violations of the statute described above in the form of:
  - a. records of or information about the SUSPECT DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in victim G.T. or the owner of Victim Phone Number;
  - b. Records and information referencing harassing phone calls;
  - c. Records and information referencing call obfuscation techniques or the use of computer-assisted callers, aka "robocall" technology;
  - d. Records and information pertaining to telephone numbers Victim Phone Number, known to law enforcement, or 732-896-1716 (SUSPECT PHONE NUMBER);

- e. Call and text message records and contents between the Victim Phone Number and the SUSPECT PHONE NUMBER or SUSPECT DEVICE or referencing the Victim Phone Number or G.T.;
- f. Records, information, and items relating to the ownership or control of the SUSPECT DEVICE;
- g. Records, information, and items relating to the ownership or control of the SUSPECT PHONE NUMBER and/or SUSPECT DEVICE;
- h. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- i. Records referencing or revealing communication or interaction between MONTERO and G.T., including the location of occurrence;
- j. Records and information that reveals the nature of the relationship, or lack thereof, between the user of 732-896-1716 (SUSPECT PHONE NUMBER) and the user of the Victim Phone Number (the specific number is known to law enforcement).
- k. Records and information that reveals the nature of the relationship, or lack thereof, between MONTERO and G.T.

The term “storage medium” includes any physical object upon which computer data can be recorded, including micro SD cards, macro SD cards, SIM cards, cellular phones capable of storage, memory cards, memory chips, and other magnetic or optical media.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records from the SUSPECT DEVICE in order to locate the things particularly described in this Warrant.